CLAIMS

1. A method for realizing data security storage by means of semiconductor memory device, comprising a semiconductor memory device, the semiconductor memory device comprising controller module as well as universal interface module and semiconductor storage medium module electrically connected with the controller module, respectively, characterized in that the method of data security storage comprises the steps of:

? dividing the semiconductor storage medium module into at least two logic memory spaces;

? using at least one of the logic memory spaces for storing the data to be protected;

? setting up and storing passwords for the semiconductor memory device and said at least one logic memory space;

? certifying the password before read/write operation;

? when writing the data to be protected in the semiconductor memory device, the controller module receiving the data from the universal interface and, after encrypting the data, storing it in the semiconductor storage medium module; and

? when reading the data to be protected from the semiconductor memory device, the controller module decrypting the data and transmitting the decrypted data via a universal interface.

2. The method for realizing data security storage by means of semiconductor memory device of claim 1, characterized in that at least one of the logic memory spaces is for storing algorithm, and the controller module executes the designated algorithm according to input data from the universal interface and transmits the operation result via the universal interface.

3. The method for realizing data security storage by means of semiconductor memory device of claim 1, characterized in that the semiconductor storage media module may be a storage medium, or combinations of at least two storage media.

4. The method for realizing data security storage by means of semiconductor

memory device of claim 1, characterized in that the semiconductor memory device and/or said at least one logic memory space set up at least two levels of users passwords.

5. The method for realizing data security storage by means of semiconductor memory device of claim 4, characterized in that certification of user passwords may be implemented before the operation in all logic memory spaces, and it may also be implemented before the operation in the logic memory spaces storing the data to be protected.

6. The method for realizing data security storage by means of semiconductor memory device of claim 1, 4 or 5, characterized by setting up a database, and conducting the access and /or authority management to the data to be protected by way of the database.

7. The method for realizing data security storage by means of semiconductor memory device of claim 6, characterized in that the authorities comprise reading, writing, modifying, deleting and executing authorities, each authority having the meanings of:

Reading authority: only allowing reading record data in the database;

Writing authority: only allowing writing new data in the database, but not covering the record data with the same record title;

Modifying authority:only allowing writing data in the database and covering the record data with the same record title;

Deleting authority: allowing deleting the database or the records therein;

Executing authority: allowing executing record codes in the database, which is an authority with respect to written data of self-defined algorithm or function code and is normally invalid to designate executing authority for record data.

8. The method for realizing data security storage by means of semiconductor memory device of claim 1, characterized in that at least one of the logic memory spaces is used for storing the data that does not need protection.

9. The method for realizing data security storage by means of semiconductor memory device of claim 1, characterized by identifying whether the transmitted

and/or stored data is falsified or not.

10. The method for realizing data security storage by means of semiconductor memory device of claim 9, characterized in that during transmitting or storing data, the anti-falsification identification comprises the steps of:

A. invoking encrypting algorithm to convert original data to obtain conversion value X;

B. packing the original data and the conversion value X according to certain format to form data package;

C. transmitting or storing the whole data package; and

during receiving and reading the data, the method comprises the steps of:

A. unpacking the data package according to the aforesaid same format to obtain the original data and the conversion value X of the original data;

B. invoking the encrypting algorithm the same as the aforesaid one to calculate conversion value of the original data to obtain conversion value Y;

C. comparing the calculated conversion value Y and the received conversion value X to see whether they are equal to each other;

D. if the compared result is equal, indicating the data that have not been falsified, and otherwise indicating the data having been falsified.

11. The method for realizing data security storage by means of semiconductor memory device of claim 1 or 9, characterized by using randomly changeable session key to encrypt the data during the data transmission.

12. The method for realizing data security storage by means of semiconductor memory device of claim 11, characterized in that the step of using randomly changeable session key to encrypt data comprises the steps of:

A. at the beginning of the data transmission, transmission end transmitting a command of exchanging session key and introducing at least one random number at the same time;

B. after receiving the exchanging session key request, the semiconductor memory device randomly creating at least one random number, converting the received random number and the created random number by the algorithm to produce a session key, and then returning the random number created by the semiconductor memory device to the transmission end;

C. after the transmission end receives the returned random number, converting the received random number and the random number introduced by the transmission end itself with the same algorithm to produce the session key.

13. The method for realizing data security storage by means of semiconductor memory device of claim 1, characterized in that the data to be protected include, but not limited to, documents, passwords, cipher keys, account numbers, digital certificates, encrypting algorithm, self-defining algorithm, user information and user self-defined data.

14. A method for realizing algorithm storage by means of semiconductor memory device, including a semiconductor memory device that comprises a controller module, and a universal interface module and a semiconductor storage medium module that are electrically connected with the controller module, respectively, characterized in that the method of algorithm storage comprises the steps of:

? dividing the semiconductor storage medium module into at least two logic memory spaces;

? using at least one of the logic memory spaces for storing an algorithm;

? the controller module receiving input data from the universal interface;

? the controller module executing the designated algorithm according to the input data, and transmitting the operation result via the universal interface.

15. The method for realizing algorithm storage by means of semiconductor memory device of claim 14, characterized in that the semiconductor storage medium module may be a storage medium, or a combination of at least two storage media.

16. The method for realizing algorithm storage by means of semiconductor memory device of claim 14, characterized in that the algorithm is an algorithm or several algorithms

17. The method for realizing algorithm storage by means of semiconductor memory device of claim 14, characterized in that the algorithm is an algorithm

built in the semiconductor memory device or self-defined algorithm.

18. The method for realizing algorithm storage by means of semiconductor memory device of claim 14, characterized by identifying whether the transmitted and /or stored data is falsified or not.

19. The method for realizing algorithm storage by means of semiconductor memory device of claim 18, characterized in that when transmitting or storing the data the anti-falsifying identification comprises the steps of:

A. invoking an encrypting algorithm to convert original data to obtain conversion value X;

B. packing the original data and the conversion value X according to certain format to form a data package;

C. transmitting or storing the whole data package; and

during receiving or reading data the method comprises the steps of:

A. unpacking the data package according to the aforesaid format to obtain the original data and the conversion value X of the original data;

B. invoking the encrypting algorithm the same as the above one to calculate conversion value of the original to obtain conversion value Y;

C. comparing the calculated conversion value Y and the received conversion value X to see whether they are equal to each other

D. if the compared result is equal, indicating that the data has not been falsified, and otherwise indicating that the data has been falsified.

20. The method for realizing algorithm storage by means of semiconductor memory device of claim 14 or 18, characterized by using a randomly changeable session key to encrypt the data during the data transmission.

21. The method for realizing algorithm storage by means of semiconductor memory device of claim 20, characterized in that the step of using randomly changeable talking cipher key to encrypt data comprises the steps of:

A. at the beginning of data transmission, transmission end transmitting a command of exchanging talking cipher key and introducing at least one random number at the same time;

B. after receiving the exchanging session key request, the semiconductor memory device creating randomly at least one random number, converting the received random number and the created random number by the algorithm to produce a session key, and then returning the random number created by the semiconductor memory device to the transmission end;

C. after the transmission end receives the returned random number, converting the received random number and the random number introduced by the transmission end itself with the same algorithm to produce the session key.